David A. LaFuria
8300 Greensboro Dr.
Suite 1200
Tysons, VA 22102

dlafuria@fcclaw.com
(703) 584-8666
www.fcclaw.com

LLGS | LUKAS LAFURIA GUTIERREZ & SACHS LLP

June 27, 2019

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, S.W., Room TW-B204
Washington, D.C. 20554

Re: WC Docket 18-89

Dear Ms. Dortch:

On June 27, 2019, Christopher Reno of Union Telephone Company participated in the stakeholder workshop titled, "Security Vulnerabilities Within Our Communications Networks: Find It, Fix It, Fund It," held at the Commission's meeting room.

A copy of Mr. Reno's remarks, as prepared for delivery, along with a presentation he referred to during his participation on the panel discussion, are enclosed.

Should you have any questions, please contact undersigned counsel directly.

Sincerely,

David A. LaFuria
Counsel for Union Telephone Company

Enclosure

cc: Hon. Geoffrey Starks
Randy Clarke, Esq.
Christopher Reno

**SECURITY VULNERABILITIES WITHIN OUR COMMUNICATIONS NETWORKS:**
**FIND IT, FIX IT, FUND IT**
Stakeholder Workshop
Federal Communications Commission
June 27, 2019

**Remarks of Christopher Reno, Chief Accounting Officer**
Union Telephone Company, Mountain View, Wyoming
(as prepared for delivery)

Good afternoon, Commissioner Starks. Thank you for leading the Commission's effort to solve a problem that, as you've heard from the earlier panels, threatens to decimate investment in mobile broadband networks, putting rural Americans even farther behind their urban counterparts.

Founded in 1914, the Union Telephone Company is a family owned and operated company, providing mobile broadband, landline telephone, and broadband services throughout vast areas in Wyoming, Northwestern Colorado, and parts of Utah, Idaho, and Montana. Our mobile broadband network includes 418 cell sites, connected with fiber and microwave, to our switch located at our Mountain View, Wyoming headquarters. To the greatest extent possible, we provide our customers with tools and capabilities that are comparable to those in urban areas and we support the FCC's goals in this regard.

Our founder, John D. Woody, was a tech leader 105 years ago when he understood the power of basic connectivity. Today, the company continues that vision, having invested over $48 million in 3G and 4G LTE broadband over the past four years, as well as $30 million to build regional fiber in remote parts of Wyoming in just the past seven years. Of that $48 million for mobile broadband, $27.5 million has been for equipment, $12.4 million has been for software, and $8.6 million has been for installation and optimization costs.

The Woody family asked me to appear before you today because when investments get made, they have to go through my office. I'm a CPA, and over a 32 year career I've been the Chief Financial Officer of the Champlain Telephone Company in New York, and am now Union's Chief Accounting Officer. I know our networks inside and out, and have spent an enormous amount of time working the finance side of the problem we are talking about today. My remarks here apply to a number of other rural broadband providers that we have been working with to solve this problem, in places like Colorado, Tennessee, American Samoa, Alaska, Oklahoma, and Kansas.

When we use the words, "rip and replace," we're not talking about replacing the battery in an automobile. A mobile broadband network is a complex web of switching equipment, known as the Core; equipment at each of our cell sites, known as the Radio Access Network or

RAN; and associated equipment to move traffic among cell sites. The Core and the RAN equipment on each tower speak to each other in a unique technical language. As of today, we cannot replace just the Core and continue to use the RAN – it all has to go.

This is a complex problem because we will need to build a parallel network on top of our existing network. Our crews will need to climb hundreds of towers to place new equipment and remove the old equipment. We can put up new equipment at a rate of approximately fifteen towers per month, and we have up to six months out of the year when the weather permits us to do this work, and we are often limited by issues on federally managed lands such as permitting and wildlife management. We estimate that a rip and replace solution will take Union approximately seven years to execute.

Importantly, it will also adversely affect our plans to continue expanding our network. As a small company in a remote region, we have limited resources. There are only so many tower climbers and there's only so many dollars available to solve this problem, to maintain our network, repair outages, and upgrade our facilities. In short, the opportunity cost of going through this exercise is enormous – every dollar and man hour spent on this project represents resources that don't expand coverage, build fiber to our towers, improve broadband in rural areas, or help our communities.

To give you a sense of the dollars, I've looked at our network and estimated the cost of replacing what we have with a network from one of the remaining vendors. If it were possible to do an immediate rip and replace, I estimate a total cost of $8 million to replace the Core, $75 million to replace the RAN, and $2 million to replace backhaul and related equipment, for a total cost of $85 million. These numbers include the cost of purchasing new equipment and the labor needed to do the work. If this replacement is extended out over a longer period, as we believe it must in order to provide time to switch out the RAN equipment, the cost will come down, depending upon the length of time given.

For a company of our size, a rip and replace solution is an extraordinary expense that we could not bear. Nor is it something that could be funded from our current universal service support, as those funds are being used for operating expenses to maintain our current network, and capital for expansion. I am confident that this is the case with respect to each of the other affected rural carriers.

Let me spend a moment to offer you a proposed solution that could be far less expensive, and much more effective, than rip and replace. We are advised by experts that there is an ocean of equipment and components currently present in our telecom and Internet ecosystem, sourced in China, likely by a company that is under the same obligations to China's government as Huawei. These components are likely present within most all major equipment manufacturer's gear, whether it be a small home router or sophisticated enterprise class equipment. In other words, ripping and replacing the equipment of a few rural mobile broadband carriers is not going to make the United States even 1% more secure from foreign influence.

We urge you to investigate the possibility of developing a mechanism that does not trust any vendor. Whether it be the FCC, through its equipment certification process, or other branches of the federal government, it is possible to set up a facility into which equipment makers submit hardware and source code for review and approval. We are advised that the cost of such a facility drops dramatically over time as it scales up, an estimated $50 million over ten years to run it. I'm attaching to my testimony a presentation we've given to Senators Warner and Rubio, in response to their briefing last month, which describes how a trusted delivery mechanism can work to secure our networks. We think it deserves your consideration.

Let me close by saying, we're patriots. Members of the Woody family have served in the United States Military since World War II. You have our commitment that we will do our part to advance the nation's best interests. There are no qualifiers on this – we're here to help and I'm happy to answer any questions you may have.

# Securing U.S. Telecommunications Networks and the Global Supply Chain

## Rural Wireless Broadband Coalition

David LaFuria
Lukas, LaFuria, Gutierrez & Sachs, LLP
8300 Greensboro Drive, Suite 1200
Tysons, VA 22102
www.fcclaw.com
703-584-8666

# Huawei Gear in Rural Networks

- Huawei 3G/4G equipment is in a number of rural carrier networks (switch, RAN, other base station, handsets)
- Equipment has been purchased over the past ten years. Upgrades and expansions have added to initial purchases
- In some cases, more than 1,000 cell sites have Huawei gear, and Huawei is used in some microwave backhaul networks
- Tearing out an entire network without significant disruption to rural citizens who depend on the network is *impossible* without significant planning and financial resources
- All carriers accept the intelligence community assessment that Huawei and other network equipment from China might present a threat to national security

# Elements Needed to Implement a Switch Out of Huawei Network Equipment for Rural Carriers

- There must be a long ramp – an exclusion period during which carriers can continue to operate existing networks while changing equipment out….ten years
- Financial assistance for equipment previously purchased (much of it financed and still in its useful life) plus the cost of rip and replace
- Financial assistance/subsidy to purchase new equipment from remaining vendors. Small carriers purchasing at small scale pay much higher prices and need some subsidy to be competitive
- Financial assistance for increased opex going forward. Remaining vendors' software licensing charges significantly depress margins and compromise small carriers' ability to compete with larger carriers

# Threats to the Global Supply Chain Must be Addressed Now to Avoid Much Larger Threats to National Security

- Telecom/Internet equipment currently distributed by so-called “trusted” vendors contain components manufactured in China (some specifically manufactured in Huawei/ZTE factories) under “white label” arrangements
- Telecom/Internet equipment contains components sourced from all over the world. Vendors typically buy components in bulk from the least-cost provider, to be delivered to an assembly factory
- **Without significant reforms to supply chain security, rip/replace for a few small rural carriers will not make the USA even one percent safer from the China threat**

# Small Carriers Cannot be Asked to Manage Global Supply Chain Risks

- There is no way for a small carrier to know whether a box contains communications components harboring malware
- Small carriers cannot vet a global supply chain to determine whether individual components are sourced from an unreliable source
- It does no good for a small carrier to tear out Huawei equipment, only to replace it with gear that contains parts manufactured by Huawei and delivered through an insecure supply chain
- Without reforms to the global supply chain, there is a legitimate fear that small carriers will find themselves in the same position they are today – having network components that represent a security risk to the USA

# What do Small Carriers Need from the Government?

- A carrier needs to be able to buy equipment from a reputable vendor with reasonable confidence that what is inside the box has been vetted for security issues and delivered through a secure supply chain, essentially a “white list” of products
- Either the government or a trusted third-party must set up a secure facility to vet equipment and software before it is distributed into US-based networks
- Vendors must be required to provide all equipment-related intellectual property and all software source code for examination
- Without such a mechanism, components that represent potentially significant risks for exfiltrating data and denial of service attacks will continue to pour into carrier, business, and home-based Internet ecosystems

# Comments on S.1625 – US 5G Leadership Act of 2019

- Important to act quickly – the proposed Aug. 14, 2018 cutoff date (§5(b)(2)) freezes network investment for affected companies *today,* just as 5G is rolling out
- §4(b)(2) exemption is critical as there are many 'dumb' network components that do not pose a threat
- §6 - $700M will be insufficient to prevent significant harm to rural carriers. Must increase the amount, broaden permissible use of funds, and authorize FCC to use other auction proceeds, or USF, to assist rural providers
- The bill should create a trusted delivery platform, recognizing that supply chains contain components manufactured by covered companies

# Small Carrier Proposal for Trusted Delivery

- In 2018, seven small rural carriers engaged a company with expertise to assist the FCC in improving supply chain security. Today, any plan must secure the supply chain by testing of hardware and software network components and creating a trusted delivery mechanism.
- The cost of setting up and operating a testing facility would be a fraction of the cost of tearing out small carrier networks and it would significantly increase overall USA supply chain and network security
- A short presentation explaining how a trusted delivery mechanism could be set up to increase supply chain security follows

# Securing Telecommunications Supply Chains: High Assurance Security Evaluation & Trusted Delivery

# Trusted Delivery Programs Reduce Supply Chain Risk

- High Assurance Independent Evaluation and Trusted Delivery programs are rigorous evidence-based risk assessments to identify and mitigate risk.

- Trusted Delivery methods, in place over the past eight years, have matured for a number of major telecom vendor technology solutions, including 3G/CDMA, LTE (TDD & FDD) and preliminary 5G implementations.

- Trusted Delivery programs are proven to address US Government telecommunications security concerns and to directly mitigate threats and reduce security risks.

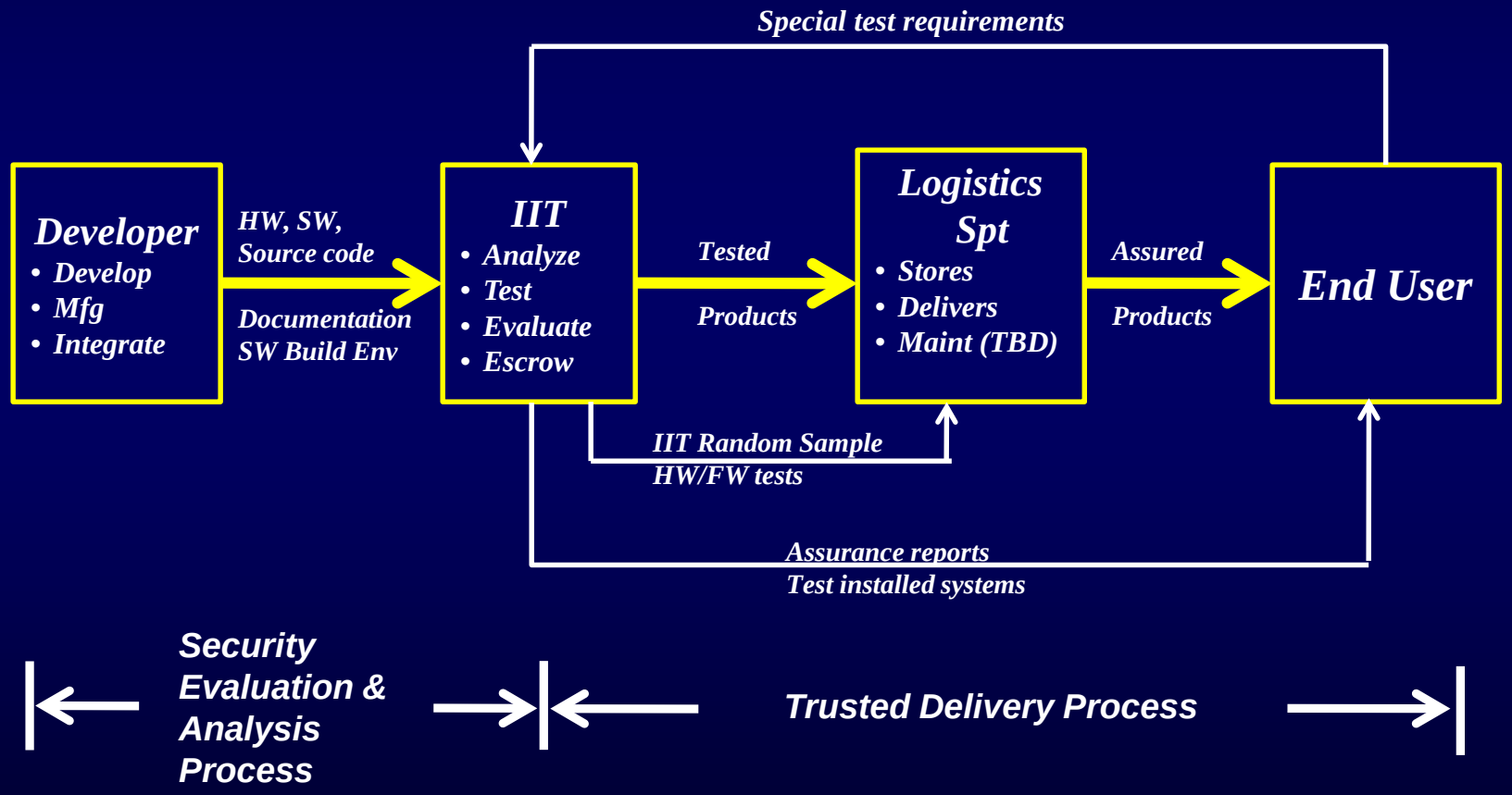
# Trusted Delivery Credibly Addresses Critical Supply Chain Security Vulnerabilities

- Provides end user assurances that systems (hardware, software and firmware) precisely match those that were fully evaluated in IIT labs
- Enabled by initial comprehensive evaluation
- Extends security assurance across the full life-cycle of the technology deployment
- Addresses patches, new releases, and upgrades
- Provides assurances against undocumented changes being made by the vendor or any third party

# Trusted Delivery Programs Bring Value to Every Stage of Supply Chain Security

- Identifies and mitigates vulnerabilities, weaknesses, and exposures not detected through conventional C&A or Security Evaluation
- Initial and follow-on lifecycle testing mapped to analyzed threats and vulnerabilities
- Continuously evaluates vulnerability to evolving and newly discovered threats
- Dramatically improves quality of software/source code, which greatly improves performance
- Forces high level of maturity and diligence in vendor development practices
- Continually saves money and resources in delivering essential cyber security protection

# The Telecommunication Systems Trusted Delivery/Supply Chain Assurance Model



# Rural Wireless Broadband Coalition Members

- Bristol Bay Cellular
- Pine Cellular Phones, Inc.
- Union Wireless
- United Wireless Communications
- Viaero Wireless
- AST Telecom
- SI Wireless